

REMARKS

The Office Action dated January 22, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

By this Response, claims 1, 5-6, 14, 17-24, and 28 have been amended to more particularly point out and distinctly claim the subject matter of the present invention. Claims 2-3 and 15-16 have been cancelled without prejudice or disclaimer. Claims 12-13 and 25-27 were previously withdrawn. No new matter has been added and no new issues are raised which require further consideration and/or search. Accordingly, claims 1, 4-11, 14, 17-24, and 28-31 are currently pending, of which claims 1, 14, and 28 are independent claims.

Applicant thanks the Examiner for considering its argument that IMSI is a permissible term because IMSI has an established meaning well-known and satisfactorily defined in literature, which provides sufficient definiteness (See Office Action on page 4). Applicant submits herewith evidence to support Applicant's argument that IMSI has an established meaning well-known in the art (See Appendix A).

In view of the above amendments and the following remarks, Applicant respectfully requests reconsideration and timely withdrawal of the pending rejections to the claims for the reasons discussed below.

Claim Rejections under 35 U.S.C. §102(a)

The Office Action rejected claims 1-3, 5-7, 9, 10, 14-16, 18-20, 22, 23, and 28-31 under 35 U.S.C. §102(a) as allegedly being anticipated by XP-002286828 (“XP”). The Office Action alleged that XP discloses or suggests every feature recited in claims 1-3, 5-7, 9, 10, 14-16, 18-20, 22, 23, and 28-31. Applicant respectfully submits that the claims recite subject matter that is neither disclosed nor suggested in XP.

Claim 1, upon which claims 2-10 and 13 depend, recites a method of generating a subscriber identifier. The method includes generating an identifier base string based on encrypting a subscriber identifying value, generating an integrity check value based on the identifier base string, and generating the subscriber identifier based on a concatenation of the identifier base string and the integrity check value. Generating the identifier base string includes binary coding of the subscriber identifying value, concatenating a random number, and performing an encryption algorithm on the concatenated binary coded subscriber identifying value and the random number for generating the identifier base string.

Claim 14, upon which claims 15-24 depend, recites a network control node for generating a subscriber identifier. The network node includes means for generating an identifier base string based on encrypting a subscriber identifying value, means for generating an integrity check value based on the identifier base string, and means for generating the subscriber identifier based on a concatenation of the identifier base string and the integrity check value. The identifier base string generating means includes means

for binary coding of the subscriber identifying value, means for concatenating a random number to the binary coded subscriber identifying value, and means for performing an encryption algorithm on the concatenated binary coded subscriber identifying value and random number for generating the identifier base string.

Claim 28, upon which claims 29-31 depend, recites a computer program product stored on a tangible medium. The computer program product includes software code, which performs, when executed by one or more processors, generating an identifier base string based on encrypting a subscriber identifying value, generating an integrity check value based on the identifier base string, and generating a subscriber identifier based on a concatenation of the identifier base string and an integrity check value. Generating the identifier base string includes binary coding of the subscriber identifying value, concatenating a random number, and performing an encryption algorithm on the concatenated binary coded subscriber identifying value and the random number for generating the identifier base string.

As will be discussed below, XP fails to disclose or suggest every feature recited in claims 1-3, 5-7, 9-11, 14-16, 18-20, 22-24, and 28-31, and therefore fails to provide the features discussed above.

XP is directed to using cookies. XP discloses that an alternative to using hidden fields or URLs is to store information such as usernames, passwords, and shopping cart contents in HTTP cookies. Users may modify the cookies; thus, cookies have the same problems encountered for hidden fields or compound URLs. Additionally, cookies have

their own problems. XP further discloses that cryptography, and more particularly a cryptographic block of information, can be used to protect the information in hidden fields, compound URLs, and cookies (XP, pages 451-452).

Applicant respectfully submits that XP fails to disclose or suggest every feature recited in claim 1, and similarly recited in claims 14 and 28. Specifically, XP fails to disclose or suggest, at least, “wherein the generating the identifier base string comprises: binary coding of the subscriber identifying value, concatenating a random number, and performing an encryption algorithm on the concatenated binary coded subscriber identifying value and the random number for generating the identifier base string” as recited in claim 1, and similarly recited in claims 14 and 28 (emphasis added).

The Office Action took the position that the features recited in claim 1, and similarly recited in claims 14 and 28, as originally recited in claim 2 are disclosed in the teachings of XP on page 452, in steps 1 and 2. However, a review of the steps described in XP for performing cryptography demonstrates that XP fails to disclose or suggest every feature recited in claim 1, and similarly recited in claims 14 and 28.

Rather, XP is specifically directed to creating a cryptographic block of stored information. Individual variables that need to be preserved are encoded into a string. A 4-byte timestamp is prepended to the variables. Data is compressed, and the length of the string is prepended to the data. The string is encrypted using a symmetric encryption function with a secret key. A HMAC function is calculated of the encrypted string and prepended to the encrypted string (XP, page 452, steps 1-6).

XP further discloses three examples, a username and password authentication, a secure shopping cart, and a compound URL, recoded to use cryptography (XP, page 451). XP further replacing the individual human-readable variables with a cryptographic block of information. In step 1, the process takes individual human-readable variables that need to be preserved and encode them as a string, i.e. marshallng. Contrary to the Office Actions' assertions, step 1 fails to disclose or suggest "binary coding of the subscriber identifying value" as recited in claim 1, and similarly recited in claims 14 and 28 (emphasis added).

Furthermore, XP discloses that a 4-byte timestamp is prepended to these variables (See step 2 on page 452). A 4-byte timestamp, which is a definite time value, is prepended to protect against replay attacks. Accordingly, XP fails to disclose or suggest, at least "concatenating a random number" as recited as recited in claim 1, and similarly recited in claims 14 and 28 (emphasis added).

Thus, XP further fails to disclose or suggest, at least, "performing an encryption algorithm on the concatenated binary coded subscriber identifying value and the random number for generating the identifier base string" as recited as recited in claim 1, and similarly recited in claims 14 and 28.

Therefore, XP fails to disclose or suggest every feature recited in claims 1, 14, and 28.

Claims 5-7 and 9-11 depend from claim 1. Claims 18-20 and 22-24 depend from claim 14. Claims 29-31 depend from claim 28. Claims 2-3 and 15-16 were cancelled

without prejudice or disclaimer. Accordingly, claims 5-7, 9-11, 18-20, 22-24, and 29-31 should be allowable for at least their dependency upon an allowable base claim, and for the specific limitations recited therein.

Therefore, Applicant respectfully requests withdrawal of the rejections of claims 1-3, 5-7, 9-11, 14-16, 18-20, 22-24, and 28-31 under 35 U.S.C. §102(a), and respectfully submit that claims 1, 14, and 28, and the claims that depend therefrom, are in condition for allowance.

Claim Rejections under 35 U.S.C. §103(a)

The Office Action rejected claims 4, 8, 14, 17, 21, and 24 under 35 U.S.C. §103(a) as allegedly unpatentable as obvious over XP. The Office Action took Official Notice, indicating that it is well known in the art to include a key identifier with encrypted data (See Office Action on pages 4-5). Applicant respectfully submits that the claims recite subject matter that is neither disclosed nor suggested in XP, nor cured by the Office's taking Official Notice that it is well known in the art to include a key identifier with encrypted data.

The Office's taking Official Notice that it is well known in the art to include a key identifier with encrypted data fails to cure the deficiencies of XP with regard to the aforementioned features recited in claims 1, 14, and 28. Specifically, the Office's taking Office Notice fails to disclose or suggest, at least, "wherein the generating the identifier base string comprises: binary coding of the subscriber identifying value, concatenating a

random number, and performing an encryption algorithm on the concatenated binary coded subscriber identifying value and the random number for generating the identifier base string” as recited in claim 1, and similarly recited in claims 14 and 28 (emphasis added). Accordingly, XP in view of the Office’s taking Official Notice fails to disclose or suggest every feature recited in claims 1, 14, and 28, and the Office’s taking Official Notice is traversed as moot.

Claims 4 and 8 depend from claim 1. Claims 17 and 21 depend from claim 14. Accordingly, claims 4, 8, 17, and 21 should be allowable for at least their dependency upon an allowable base claim, and for the limitations recited therein.

Therefore, Applicant respectfully requests withdrawal of the rejections of claims 4, 8, 17, and 21 under 35 U.S.C. §103(a), and respectfully submits that claims 1 and 14, and the claims that depend therefrom, are in condition for allowance.

CONCLUSION

In conclusion, Applicant respectfully submits that XP and the Office’s taking Official Notice that it is well known in the art to include a key identifier with encrypted data, alone or in combination, fail to disclose or suggest every feature recited in claims 1, 4-11, 14, 17-24, and 28-31. The distinctions previously noted are more than sufficient to render the claimed invention unanticipated and non-obvious. It is therefore respectfully requested that all of claims 1, 4-11, 14, 17-24, and 28-31 be allowed, and this present application be passed to issuance.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Brad Y. Chin
Registration No. 52,738

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

BYC:dlh

Enclosures: Petition for Extension of Time
Check No. 018848